Some Applications of Transcendence Theory to Linearly Recurring Sequences (数論 : Diophantine Problem)

AUTHOR(S):

KUBOTA, KENNETH K.

CITATION:

KUBOTA, KENNETH K.. Some Applications of Transcendence Theory to Linearly Recurring Sequences (数論 : Diophantine Problem). 数理解析研究所講究録 1978, 334: 11-26

ISSUE DATE:

1978-10

URL:

http://hdl.handle.net/2433/104192

数理解析研究所講究録
334巻 1978年 11-26

SOME APPLICATIONS OF TRANSCENDENCE THEORY TO LINEARLY RECURRING SEQUENCES

K. K. KUBOTA
UNIVERSITY OF KENTUCKY
TOKYO UNIVERSITY

Our purpose here is to state several natural conjectures about the behavior of linearly recurring sequences and to show how results, originally developed for use in transcendence theory, can be used to verify special cases of these conjectures.

1. Definitions.

Let us begin by setting up the notation which will be used below. A linear recurrence is defined to be a sequence $\{a_n\}_{n\geq 0}$ of algebraic integers not all zero which satisfy a recursion relation of the form

(1) $$a_{n+\sigma} = M_1 a_{n+\sigma-1} - M_2 a_{n+\sigma-2} + \ldots + (-1)^{\sigma-1} M_\sigma a_n$$

for all $n \geq 0$. Clearly, the sequence $\{a_n\}$ is determined by (1) and the initial values $a_0, a_1, \ldots, a_{\sigma-1}$. The order of the recurrence $\{a_n\}$ is the least integer σ for which a relation of the form (1) holds. In this case, the M_i are uniquely determined, and

(2) $$f(X) = X^\sigma - M_1 X^{\sigma-1} + \ldots + (-1)^\sigma M_\sigma = \prod_{r=1}^{R} (X - \beta_r)^{\sigma_r+1}$$

is called the characteristic polynomial of $\{a_n\}$; the roots $\beta_1, \beta_2, \ldots, \beta_R$ of $f(X) = 0$ are called the characteristic roots of $\{a_n\}$. If none of the characteristic roots and none of their ratios are roots of unity, then $\{a_n\}$ is said to be non-degenerate. By replacing $\{a_n\}$ with a set of subrecurrences $\{a_{rn+i}\}_{n\geq 0}$ $(0 \leq i < r)$, it is usually possible to reduce questions about general recurrences to ones about non-degenerate recurrences.

From the recurrence relation (1), it is easily verified that

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(X^\sigma f(X^{-1})\right) = g(X)$$

is a non-zero polynomial of degree less than σ. Conversely, the

Taylor series coefficients of a function of the form $g(X)/(X^{\sigma}f(X^{-1}))$ satisfy the recurrence relation (1). On the other hand, using (2) to expand $g(X)/(X^{\sigma}f(X^{-1}))$ in partial fractions, one obtains the closed formula

$$a_n = \sum_{r=1}^{R} g_r(n)\beta_r^{\,n} \tag{3}$$

where the g_r are polynomials of degree ρ_r. Thus, the three notions of linear recurrence, power series expansion of rational functions, and exponential polynomial are equivalent. In particular, it follows that $\{a_{rn+i}\}_{n\geq 0}$ is either a linear recurrence or the identically zero sequence.

Examples. (i) If g is a non-zero polynomial, then $\{g(n)\}_{n\geq 0}$ is a linear recurrence. The linear recurrences of order one are those of the form $\{g\beta^n\}_{n\geq 0}$ with g a constant.

(ii) If the characteristic polynomial f(X) has no multiple roots then $\{a_n\}$ is an exponential sum

$$a_n = \sum_{r=1}^{R} g_r\beta_r^{\,n}, \tag{4}$$

i.e. a linear polynomial in $\beta_1^{\,n}, \beta_2^{\,n}, \ldots, \beta_R^{\,n}$. In the special case where R = 2, we say that $\{a_n\}$ is a binary recurrence. We say that $\{a_n\}$ is decomposable if it is a "product of binary recurrences". More precisely, let G be a finitely generated subgroup of $\bar{\mathbb{Q}}^n$ containing $\beta_1, \beta_2, \ldots, \beta_R$; so $G = \langle\zeta\rangle \times \langle\gamma_1\rangle \times \ldots \times \langle\gamma_s\rangle$ where ζ is a root of unity and $\gamma_1, \gamma_2, \ldots, \gamma_s$ are multiplicatively independent. If k is a positive integer with $\zeta^k = 1$, then one can write

$$a_{kn+i} = F_i(\gamma_1^{\,kn}, \ldots, \gamma_s^{\,kn})/M(\gamma_1^{\,kn}, \ldots, \gamma_s^{\,kn})$$

for $0 \leq i < k$ where F_i is a polynomial and M is a monomial. Then $\{a_n\}$ is said to be decomposable if each polynomial $F_i(X_1, \ldots, X_s)$ can be factored as a product of (monomials and) binomials. Using the structure of subgroups of finitely generated free Abelian groups [3], it is easy to check that this definition does not depend on the particular choice of G, ζ, γ_i, k, F_i, or M.

The above classes of recurrences are those to which most of the

results below are applicable. Note that, if the characteristic roots of $\{a_n\}$ are of the form

(5) $$\beta_r = \beta\gamma_r^u \qquad (u_r \in \mathbb{Z},\ r = 1, \ldots, R),$$

then the sequence is decomposable by the fundamental theorem of algebra; in particular, binary recurrences are decomposable. Another example of a decomposable recurrence is

(6) $$a_n = \sum_{r=1}^{4} \beta_r^n$$

where $\beta_1 = \overline{\beta}_2$, $\beta_3 = \overline{\beta}_4$ (complex conjugates), and $|\beta_r| = b$ for all r; using $Z = b$, $X = \beta_1/b$, and $Y = \beta_3/b$, the fact that $\{a_n\}$ is decomposable follows from the factorization

$$ZX + ZX^{-1} + ZY + ZY^{-1} = Z(XY + 1)(X + Y)/(XY).$$

2. Growth of Linear Recurrences.

The case where $\{a_n\}$ has only one characteristic root (R = 1) suggests that the following might hold.

Conjecture 1. If $\{a_n\}$ is a non-degenerate linear recurrence, then for every $\varepsilon > 0$ and $n > N(\varepsilon)$ one has

(7) $$|a_n| > \max(|\beta_1|, \ldots, |\beta_R|)^{(1-\varepsilon)n}$$

Suppose henceforth that the characteristic roots of $\{a_n\}$ are ordered in such a way that

$$\delta = |\beta_1| = |\beta_2| = \ldots = |\beta_T| > |\beta_{T+1}| \geq |\beta_{T+2}| \geq \ldots \geq |\beta_R|$$

and

$$\rho = \rho_1 = \rho_2 = \ldots = \rho_S > \rho_{S+1} \geq \rho_{S+2} \geq \ldots \geq \rho_T.$$

Then, for every sufficiently large $t \in \mathbb{N}^+$, the inequality (7) holds for at least one integer n in the interval $[t, t + S)$. This is a consequence of Turan's Third Main Theorem [17, pp. 53-56]:

Theorem A (Turan). Let $\alpha_1, \ldots, \alpha_S$ be non-zero complex numbers in the closed unit disc and set $\Delta = \min_{i \neq j}(1, |\alpha_i - \alpha_j|)$. If $g_1, \ldots, g_S$ are complex numbers not all zero, then

$$\max_{n \in [t, t+S)} \frac{\left|\sum_{r=1}^{S} g_r \alpha_r^n\right|}{\sum_{r=1}^{S} |g_r||\alpha_r|^n} \geq \frac{\Delta^{S-1}}{S2^S}$$

or all $t \in \mathbb{N}^+$.

Applied with $\alpha_r = \beta_r/|\beta_r|$ for $r = 1, \ldots, S$, Theorem A shows hat

$$\max_{n \in [t, t+S)} |a_n| \geq c^{-1} t^{\rho} \delta^t$$

or some $c > 0$ and all sufficiently large $t \in \mathbb{N}^+$.

Note that without the hypothesis that $\{a_n\}$ be non-degenerate, conjecture 1 is false; for example, the degenerate recurrence $\{a_n\}$ where

$$a_{n+2} = a_{n+1} - a_n, \; a_0 = 0, \; a_1 = 1$$

satisfies $a_{3n} = 0$ for all $n \geq 0$. On the other hand, if $\{a_n\}$ is non-degenerate, then Theorem 5 below says that no number can occur infinitely often in $\{a_n\}$.

Let $\{a_n\}$ be a non-degenerate linear recurrence whose characteristic polynomial has no multiple roots, i.e. one of the form (4). With T as above, to verify (7), it suffices to prove the analogous inequality with

$$a_n' = \sum_{r=1}^{T} g_r \beta_r^n$$

in place of $\{a_n\}$. Mahler [7] used Ridout's p-adic version of Roth's Theorem to do this for second order linear recurrences. More recently, Mignotte [8, 9] generalized this result to linear recurrences of rational integers with $T \leq 3$, by using a version of Baker's Theorem together with a trigonometric identity.

An appropriate version [1] of Baker's Theorem is the following.

Theorem B. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with heights at most $A_1, \ldots, A_n$ (≥ 4) respectively, and set

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n), \; D = [K:\mathbb{Q}], \; \Omega' = \prod_{j=1}^{n-1} \log A_j, \text{ and } \Omega = \Omega' \log A_n.$$

Then there are effectively calculable constants $c_1, c_2 > 0$ such that the inequality

$$0 < |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| < B^{-(c_1 n D)^{c_2 n}} \Omega \log \Omega'$$

has no solutions in integers $b_1, \ldots, b_n$ such that $|b_i| \leq B$ $(B \geq 4)$ for all i.

Theorem 1. With the above notation, suppose that the linear recurrence $\{a_n'\}$ is decomposable. Then there is a real number $c > 0$ depending only on $\{a_n\}$ that for all $n > 1$, one has

$$|a_n| > \max(|\beta_1|, \ldots, |\beta_R|)^{n_n - c}$$

whenever $a_n' \neq 0$. In particular, Conjecture 1 holds in case $\{a_n'\}$ is non-degenerate and decomposable.

Proof. Since $\{a_n'\}$ is decomposable, there is a k such that one has

$$a'_{kn+i} = A_{0i}\delta^{kn} \prod_{j=1}^{J} (A_{ji}a_j^{kn} - 1)$$

for $0 \leq i < k$, $n \geq 0$ where $\delta = \max(|\beta_1|, \ldots, |\beta_R|)$ and $|a_j| = 1$ for all j. The result now follows by applying Theorem B to each of the expressions $A_{ji}a_j^{kn} - 1$ $(j = 1, \ldots, J)$.

Theorem 1 explains the above mentioned result of Mignotte since $T = 3$ and $\{a_n\}$ real imply that the characteristic roots are of the form

$$\beta_1 = \delta e^{i\theta}, \quad \beta_2 = \delta e^{-i\theta}, \quad \beta_3 = \pm\delta$$

and so $\{a_n'\}$ is decomposable by (5) above. Mignotte [8,9] also verified Theorem 1 in the special case of the linear recurrence (6) which, as we have seen, is also decomposable.

3. Divisibility.

The natural $\mathcal{Y}$-adic generalization of Conjecture 1 can be stated as follows.

Conjecture 2. Let $\{a_n\}$ be a non-degenerate linear recurrence of rational integers and $p_1, \ldots, p_M$ be rational primes satisfying $(p_m, \beta_r) = 1$ for all m and r. Then, for every $\varepsilon > 0$ and $n > N(\varepsilon, p_1, \ldots, p_M)$, one has

$$\left| \frac{a_n}{\prod_{m=1}^{M} p_m^{\operatorname{ord}_{p_m} a_n}} \right| > \max\,(|\beta_1|, \ldots, |\beta_R|)^{(1-\varepsilon)n}.$$

The $\mathfrak{P}$-adic analogue of Theorem B is as follows.

Theorem C (Van der Poorten [19]). Let $\alpha_1, \ldots, \alpha_n, A_1, \ldots, A_n$ $(\geqslant e^e)$, Ω, K, and D be as in the statement of Theorem B and $\mathfrak{P}$ be a prime of K lying over the rational prime p. Then the inequality

$$\infty > \operatorname{ord}_{\mathfrak{P}} (\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1) > (16(n+1)D)^{12(n+1)} \frac{p^D}{\log p} \Omega (\log B)^2$$

has no solutions in integers $b_1, \ldots, b_n$ such that $|b_i| \leq B$ $(B \geqslant e^e)$ for all i.

Using Theorem C in place of Theorem B in the proof given for Theorem 1, one obtains the following result.

Theorem 2. Let $\{a_n\}$ be a decomposable linear recurrence. Then there is a $c > 0$ such that for every $n > 1$ either $a_n = 0$ or else

$$|a_n|_{\mathfrak{P}} > n^{-cp^D \log n}$$

for every prime $\mathfrak{P}$ of K such that $\beta_1, \ldots, \beta_R$ are $\mathfrak{P}$-adic units.

Since $\{a_n'\}$ is decomposable whenever $\{a_n\}$ is decomposable, Theorems 1 and 2 together give the following result.

Corollary. Conjecture 2 holds for all decomposable non-degenerate linear recurrences of rational integers.

Polya [10] has shown that if $\{a_n\}$ is a non-degenerate linear recurrence such that the set of prime divisors of $\{a_n\}$ is a finite set, then $\{a_n\}$ is of order one. In fact, one expects that

$$\lim_{n \to \infty} P(a_n) = \infty$$

where

$$P(a_n) = \max \{ N_{K/\mathbb{Q}} \mathfrak{P} \mid \mathfrak{P} | a_n \text{ for some } n \}.$$

Conjecture 3. If $\{a_n\}$ is a non-degenerate linear recurrence, then

$$P(a_n) \gg \text{loglog } n$$

unless $\{a_n\}$ is of the form

$$a_n = A(n - a)^m \beta^n.$$

In the case where $\{a_n\}$ has only one characteristic root ($R = 1$), this has been verified by Tijdeman and Shorey [13] using Baker's method. Also, Schinzel [11] has shown that $P(a_n) \gg n^c$ for some $c > 0$ whenever $\{a_n\}$ is a binary recurrence.

Theorem 3. Let $\{a_n\}$ be a decomposable non-degenerate linear recurrence of order greater than one. Then

$$P(a_n) \gg n^c$$

where $c > 0$ depends only on the recurrence $\{a_n\}$.

Proof. Let β be an algebraic integer with $(\beta) = (\beta_1, \ldots, \beta_R)$ and suppose that a_n satisfies (4). Define

$$b_n = \sum_{r=1}^{R} g_r (\beta_r/\beta)^r = a_n/\beta^n \quad \text{and} \quad c_n = N_{K(\beta)/\mathbb{Q}}\, b_n.$$

Since Theorem 2 can be applied to each of the conjugates of $\{b_n\}$, it is clear that the characteristic roots of $\{c_n\}$ have no common prime divisor. Also,

$$P(a_n)^{[\mathbb{Q}(\beta):\mathbb{Q}]} \geq P(c_n),$$

and so we may assume at the outset that $(\beta_1, \ldots, \beta_R) = 1$ and that $\{a_n\} \subseteq \mathbb{Z}$. Choose $c > 0$ small enough so that

$$(\log n)^2 \sum_{p < n^c} p^D \ll (\log n)^2 n^{c(D+1)} = o(n).$$

Then, by Theorems 1 and 2, a_n must be divisible by a prime larger than n^c for all sufficiently large integers n.

Let A and B be relatively prime algebraic integers. A prime $\mathfrak{P}$ of

$\mathfrak{Q}(A, B)$ is called a primitive divisor of $A^n - B^n$ if $\mathfrak{p} \mid A^n - B^n$ and $\mathfrak{p} \nmid A^m - B^m$ for all $m < n$. Using elementary methods, Birkhoff and Vandiver [2] showed that, if $A, B \in \mathbb{Z}$, then $A^n - B^n$ has a primitive prime divisor for all $n > 6$ provided that $(A, B) = 1$ and $A \neq \pm B$. As an immediate corollary, it follows that for every $m > 0$ there is a prime $p \equiv 1 \pmod{m}$ (Let $A = 2$, $B = 1$, and $n = 7m$).

Theorem 4 (Schinzel [12]). Let A and B be relatively prime algebraic integers such that A/B is not a root of unity and $AB \neq 0$. Then $A^n - B^n$ has a primitive prime divisor for every $n > c$ where $c = c([\mathfrak{Q}(A/B):\mathfrak{Q}]) > 0$ is effectively calculable.

In fact, Stewart [14] has refined Schinzel's argument to show that one can take

$$c = \max\,(2(2^d - 1),\ e^{452}d^{67})$$

where $d = [\mathfrak{Q}(A/B):\mathfrak{Q}]$.

Proof of Theorem 4 (Sketch). Let $\Phi_n(X, Y)$ be the n^{th} cyclotomic polynomial written as a binary form, $K = \mathfrak{Q}(A, B)$, and $d = [K:\mathfrak{Q}]$. Schinzel proves the following main lemma by elementary means.

Lemma. Let $\mathfrak{p} \mid \Phi_n(A, B)$ where $\mathfrak{p}$ is a prime of K and $n > 2(2^d - 1)$. If $\mathfrak{p}$ is not a primitive prime divisor of $A^n - B^n$, then $\operatorname{ord}_{\mathfrak{p}} \Phi_n(A, B) \leq \operatorname{ord}_{\mathfrak{p}} n$. In particular, $A^n - B^n$ has a primitive prime divisor whenever

$$|N_{K/\mathfrak{Q}} \Phi_n(A, B)| > n^{[K:\mathfrak{Q}]}.$$

Write $A/B = \alpha/\beta$ where $\alpha, \beta \in K$ and $(\alpha, \beta) = \mathfrak{L}$. Using

$$\Phi_n(X, Y) = \prod_{m \mid n} (X^m - Y^m)^{\mu(n/m)};$$

one obtains

$$(8)\quad \begin{cases} \dfrac{d}{[\mathfrak{Q}(A/B):\mathfrak{Q}]} \log |N_{K/\mathfrak{Q}} \Phi_n(A, B)| \\ \qquad = \displaystyle\sum_{\sigma} \sum_{m \mid n} \mu(n/m) \log |\sigma(\alpha)^m - \sigma(\beta)^m| - \varphi(n)\, N_{K'/\mathfrak{Q}} \mathfrak{L} \end{cases}$$

where $K' = \mathbb{Q}(A/B)$ and σ ranges through the isomorphisms of K' into $\mathbb{C}$. We want to apply the lemma. Using an estimate for $|\sigma(\alpha)^m - \sigma(\beta)^m|$ as in Theorem 1, one sees that in order to give a suitable lower bound for (8), it suffices to show that

$$w(\alpha, \beta) \gg_d 1 \tag{9}$$

where

$$w(\alpha, \beta) = \log \prod_{\sigma} \max(|\sigma(\alpha)|, |\sigma(\beta)|) - \log |N_{K'/\mathbb{Q}} \Sigma|.$$

But, if α/β is not an algebraic integer, then

$$w(\alpha, \beta) \geq \log |N_{K'/\mathbb{Q}} \beta / N_{K'/\mathbb{Q}} \Sigma| \geq \log 2;$$

and, if α/β is an algebraic integer, then

$$w(\alpha, \beta) \geq \max_{\sigma} \log |\sigma(\alpha/\beta)|.$$

Thus, to verify (9), it suffices to note that there are but finitely many algebraic integers γ of degree $\leq d$ which are not roots of unity and have no conjugates outside the disc of radius 2 about the origin. For further details, consult [12].

4. Multiplicity of Linear Recurrences.

Let $F(z) = \sum_{r=1}^{R} p_r(z) e^{\omega_r z}$ be an exponential polynomial where the p_r are polynomials of degree $\rho_r \geq 0$. Let $\rho > 0$ be a real number, and define the quantities

$$\sigma = \sum_{r=1}^{R} (\rho_r + 1) \quad \text{and} \quad \Omega = \max_r |\omega_r|.$$

Mahler [21] gave estimates for the number $N(F, \rho)$ of zeros of F in the disc $|z| \leq \rho$ in terms of σ, Ω, ρ, and $\Delta = \min_{r \neq s} |\omega_r - \omega_s|$. In answer to a problem of Turan, Tijdeman [16] showed that $N(F, \rho)$ could be bounded independently of Δ. In fact, he showed the following result.

Theorem D (Tijdeman). $n(F, \rho) \leq 2(\sigma - 1) + 5\rho\Omega$.

Since $\mathbb{Z}$ lies in the $\mathfrak{p}$-adic unit disc, one expects that a $\mathfrak{p}$-adic version of Theorem D would be useful in bounding the number of times zero occurs in a linear recurrence, Such results have been proved

by Laxton [5], Waldschmidt [20], and others. Van der Poorten [18] simplified the argument as follows.

Theorem E (Van der Poorten). Let $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of a number field K at a prime $\mathfrak{p}$ lying over the rational prime p. Let $F(z) = \sum_{r=1}^{R} p_r(z)\, e^{\omega_r z}$ where the $\omega_r \in K_\mathfrak{p}$ are distinct and the $p_r(z)$ are non-zero polynomials in $K_\mathfrak{p}[z]$ of degree ρ_r. Suppose that $\operatorname{ord}_p \omega_r \geqslant (p-1)^{-1} + \varepsilon$ $(\varepsilon > 0)$, and set $\sigma = \sum_{r=1}^{R} (\rho_r + 1)$. Then the number of zeros of $F(z)$ in $K_\mathfrak{p}$ with $|z|_\mathfrak{p} \leq 1$ is less than

$$(\sigma - 1)(1 + ((p-1)\varepsilon)^{-1}).$$

The proof depends on the following simple case of the $\mathfrak{p}$-adic version of the Weierstrass Preparation Theorem.

Lemma (Strassman [15]). Let $\pi \in K_\mathfrak{p}$ be such that $\operatorname{ord}_\mathfrak{p} \pi = 1$, and $F(z) = \sum_{k=0}^{\infty} f_k(z)\pi^k \in K_\mathfrak{p}[[z]]$ where the $f_k(z)$ are polynomials whose coefficients are $\mathfrak{p}$-adic units and $f_0 \not\equiv 0$. Then $F(z) = G(z)H(z)$ where $G(z)$ is a polynomial of degree $\deg f_0$, H is a power series with $H(0) = 1$, and the coefficients of G and H are $\mathfrak{p}$-adic integers. In particular, the equation $F(z) = 0$ has at most $\deg f_0$ solutions in $\overline{K}_\mathfrak{p}$ with $|z|_\mathfrak{p} \leq 1$.

Proof. Write $\sum f_k \pi^k = (\sum g_i \pi^i)(\sum h_j \pi^j) = \sum \pi^k \sum_{i=0}^{k} g_i h_{k-i}$.

Letting $h_0 = 1$ and $g_0 = f_0$, one can solve successively for g_i, h_i with $\deg g_i < \deg g_0$ using the division algorithm for polynomials. If $|z|_\mathfrak{p} \leq 1$, then $H(z)$ is a $\mathfrak{p}$-adic unit, and so $F(z) = 0$ only if $G(z) = 0$. Since G is a polynomial of degree $\deg f_0$, it follows that $F(z) = 0$ has at most $\deg f_0$ $\mathfrak{p}$-adic integer roots.

Proof of Theorem E. By elementary calculus, we know that F is a solution of the differential equation

$$D^\sigma F = c_1 D^{\sigma-1} F + \ldots + c_\sigma F$$

where $DF = dF/dz$ and

$$\prod_{r=1}^{R} (X - \omega_r)^{\rho_r+1} = X^{\sigma} - c_1 X^{\sigma-1} - \ldots - c_{\sigma}.$$

Letting

$$F(z) = \sum_{h=0}^{\infty} a_h z^h = \sum_{h=0}^{\infty} b_h z^h/h!$$

where we may assume that $\min_h \operatorname{ord}_{\mathfrak{z}} a_h = 0$, we have

$$D^i F = \sum_{h=0}^{\infty} b_{h+i} z^h/h!$$

and so

$$b_{h+\sigma} = c_1 b_{h+\sigma-1} + \ldots + c_{\sigma} b_h \tag{10}$$

for $h \geqslant 0$.

Since $\operatorname{ord}_p \omega_r \geqslant (p-1)^{-1} + \varepsilon = q$ and $\operatorname{ord}_p b_h \geqslant 0$, it follows that $\operatorname{ord}_p c_i \geqslant q$, and so $\operatorname{ord}_p b_{h+\sigma-1} \geqslant qh$ by (10). But then

$$\operatorname{ord}_p a_{h+\sigma-1} = \operatorname{ord}_p b_{h+\sigma-1} - \operatorname{ord}_p (h+\sigma-1)!$$

$$\geqslant qh - (h+\sigma-1)/(p-1) = ((p-1)^{-1} + \varepsilon)h - (h+\sigma-1)/(p-1)$$

$$= \varepsilon h - (\sigma-1)/(p-1) > 0 \text{ if } h \geqslant (\sigma-1)/(\varepsilon(p-1)).$$

Thus $\operatorname{ord}_p a_n > 0$ if $n \geqslant (\sigma-1)/(\varepsilon(p-1)) + \sigma - 1 = (\sigma-1)(1+(\varepsilon(p-1))^{-1})$. Therefore, Theorem E follows from Strassman's Lemma.

The <u>multiplicity</u> μ <u>of a linear recurrence</u> $\{a_n\}$ is defined by

$$\mu = \sup_{c \in \bar{\mathbb{Q}}} \text{Card.}\{ n \mid a_n = c\}.$$

We have already seen an example of a degenerate recurrence with infinite multiplicity. On the other hand, using elementary calculus, it is a straightforward exercise to show that, if all the characteristic roots of a linear recurrence are real, then it has multiplicity at most equal to its order.

<u>Theorem 5</u> (Skolem, Mahler [6]). Every non-degenerate linear recurrence $\{a_n\}$ has finite multiplicity. In particular, if $\{a_n\}$ is a non-degenerate integer recurrence, then $\lim_{n\to\infty} |a_n| = \infty$.

<u>Proof</u>. Let $\mathfrak{z}$ be a prime with $\mathfrak{z} \nmid \prod_{r=1}^{R} \beta_r$ and $d \in \mathbb{N}^+$ be such that

$|\beta_i^d - 1|_p < p^{-(p-1)^{-1}}$. Now apply Theorem E to each subrecurrence $\{a_{dn+i}\}_{n\geq 0}$ with $0 \leq i < d$.

In the thirties, Ward conjectured that $\mu \leq 5$ for every non-degenerate second order integer recurrence. In fact, using the argument of Theorem 5 with a more complicated scheme for choosing an appropriate prime $\wp$, it has been shown [4] that the following is true.

Theorem 6. $\mu \leq 4$ for every non-degenerate second order linear recurrence of rational integers.

An extreme example is the sequence $\{a_n\}$ where

$$a_{n+2} = -a_{n+1} - 2a_n,\ a_0 = 0,\ a_1 = 1$$

which has $a_2 = a_3 = a_5 = a_{13} = -1$.

Various authors have conjectured that the following must hold.

Conjecture 4. The multiplicities of non-degenerate linear recurrences in a number field K are uniformly bounded in terms of their orders and the degree $[K:\mathbb{Q}]$.

We have already remarked that this is true if the characteristic roots are all real.

Theorem 6. Let $\{a_n\}$ be a non-degenerate linear recurrence in a number field K whose characteristic polynomial has no multiple roots and whose characteristic roots are of the form

$$\beta_r = \beta\gamma^{u_r} \qquad (u_r \in \mathbb{Z},\ r = 1, \ldots, R)$$

where β and γ are algebraic. If $c \in \overline{\mathbb{Q}}^x$, then the number of solutions of $a_n = c$ is bounded by a number effectively calculable in terms of the order σ of $\{a_n\}$, the degree $[\mathbb{Q}(\gamma):\mathbb{Q}]$, $u = \max_r |u_r|$, and the number of prime divisors in $\mathbb{Q}(\gamma,c)$ of c which do not divide $\gamma - 1$.

Proof. Let $a_n = \sum_{r=1}^{R} g_r \beta_r^n$ and suppose that there is a $v \in \mathbb{N}^+$ and a

prime $\mathfrak{p}$ with

$$\operatorname{ord}_{\mathfrak{p}} (\gamma^v - 1) \geq 2/(p-1), \quad \operatorname{ord}_{\mathfrak{p}} g_r \geq 0, \text{ and } \operatorname{ord}_{\mathfrak{p}} \beta = \operatorname{ord}_{\mathfrak{p}} c = 0.$$

Let w be the multiplicative order of $\beta^v \pmod{p^{2/(p-1)}}$. Then

$$a_{vwn+vj+i} \equiv \Big(\sum_{r=1}^{R} g_r \gamma^{u_r i}\Big) \beta^{i+vj} \pmod{p^{2/(p-1)}}$$

for $n \geq 0$ where $0 \leq i < v$ and $0 \leq j < w$. Thus, if c occurs in $\bigcup_{j=0}^{w-1} \{a_{vwn+vj+i}\}_{n\geq 0}$, then $\sum_r g_r \gamma^{u_r i} \not\equiv 0 \pmod{\mathfrak{p}}$ and c occurs in precisely one of these w subrecurrences. By Theorem E, it follows that $a_n = c$ has less than $v(\sigma - 1)(3/2)$ solutions. Thus, we need only find an upper bound for v.

Let $\gamma = A/B$ where $(A, B) = 1$ and A, B are algebraic integers. We know γ is not a root of unity since $\{a_n\}$ is non-degenerate. We will take for $\mathfrak{p}$ a certain primitive prime divisor of $A^v - B^v$.

Since the ramification index of $\mathfrak{p}$ is at most $d = [\mathbb{Q}(\gamma):\mathbb{Q}]$, one has $\operatorname{ord}_{\mathfrak{p}}(\gamma^v - 1) \geq 2/(p-1)$ except when $p \leq 2d$. Further, we have made an exception of no more than $2d^2$ primes .

By Cramer's rule applied to

$$\sum_{r=1}^{\sigma} g_r \beta_r^j = a_j \quad (j = 0, 1, \ldots, \sigma - 1),$$

we know that Δg_r is an algebraic integer for all r where

$$\Delta = \det (\beta_r^j)_{r,j} = \prod_{s,t} \beta(\gamma^{u_s} - \gamma^{u_t}).$$

Thus, if $\operatorname{ord}_{\mathfrak{p}} \beta = 0$ and $2(2u)! \mid v$, then $\operatorname{ord}_{\mathfrak{p}} g_r \geq 0$ for all r since $\mathfrak{p}$ is a primitive prime divisor.

Now we may assume that any prime divisor of $(\beta_1, \ldots, \beta_R)$ also divides c. In fact, $\mathfrak{p} \mid a_n$ for all $n \geq \sigma$ by the recurrence relation. Thus, $\mathfrak{p} \nmid c \Rightarrow a_n \neq c$ for $n \geq \sigma$. In particular, $\operatorname{ord}_{\mathfrak{p}} (\gamma^v - 1) > 0$ and $\operatorname{ord}_{\mathfrak{p}} \beta > 0$ implies $\mathfrak{p} \mid c$. Thus, in order to fulfill all the conditions on $\mathfrak{p}$ we need only avoid those primes dividing c but not $\gamma - 1$ and at most $2d^2$ additional primes. If this gives a total of P primes in all, then we can choose $\mathfrak{p}$ from amongst the primitive prime divisors of $A^v - B^v$ where v ranges through the first P + 1 multiples of $2(2u)!$ larger than c where $c = c(d)$ is as in the statement of Theorem 4.

Corollary. The multiplicity of a non-degenerate second order linear recurrence $\{a_n\}$ is bounded above by a number depending only on $[\mathbb{Q}(\beta_1/\beta_2):\mathbb{Q}]$.

Proof. It suffices to bound the number of occurrences of a_0 in $\{a_n\}$. Let a, b be algebraic integers satisfying

$$a = (a_0, a_1) \text{ and } b = (\beta_1, \beta_2),$$

and define $\bar{\beta}_r = \beta_r/b$, $\bar{a}_n = a_n b^{1-n}/a$. One readily verifies that

$$a_n = \frac{\beta_1^n - \beta_2^n}{\beta_1 - \beta_2} a_1 - \beta_1\beta_2 a_0 \frac{\beta_1^{n-1} - \beta_2^{n-1}}{\beta_1 - \beta_2} \quad \text{for } n > 0$$

and the analogous formula with $\bar{\beta}_r$, $\bar{a}_n$ in place of β_r, a_n respectively. Since $ab^{n-1} \mid a_n$ for $n \geq 2$, we may assume that $ab \mid a_0$ (or else $a_n \neq a_0$ for $n \geq 2$). One has

$$(11) \qquad \bar{a}_n \equiv \frac{\bar{\beta}_1^n - \bar{\beta}_2^n}{\bar{\beta}_1 - \bar{\beta}_2} \bar{a}_1 \pmod{\bar{a}_0} \quad \text{for } n > 0.$$

Let $m = \inf \{n \mid (\bar{\beta}_1^n - \bar{\beta}_2^n)/(\bar{\beta}_1 - \bar{\beta}_2) \equiv 0 \pmod{\bar{a}_0}\}$. Since $a_n \neq a_0$ for $n > 0$ if $m = \infty$, we may assume that $m < \infty$. We have by (11) that

$$\bar{a}_n \equiv 0 \pmod{\bar{a}_0} \iff \frac{\bar{\beta}_1^n - \bar{\beta}_2^n}{\bar{\beta}_1 - \bar{\beta}_2} \equiv 0 \pmod{\bar{a}_0} \iff m \mid n.$$

Further, for any prime $\mathfrak{p}$, one has

$$\mathfrak{p} \mid \bar{a}_0 \Rightarrow \mathfrak{p} \nmid \bar{\beta}_1\bar{\beta}_2 \;\&\; (\beta_1/\beta_2)^m \equiv 1 \pmod{\mathfrak{p}}$$

by the choice of m. Thus the result follows from Theorem 6 applied to $\{\bar{a}_{mn}\}_{n\geq 0}$, $c = \bar{a}_0$, and $\gamma = (\beta_1/\beta_2)^m$.

REFERENCES

1. A. Baker, The theory of linear forms in logarithms, in "Advances in Transcendence Theory", Academic Press, London, 1978.

2. G. Birkhoff and H. Vandiver, On the integral divisors of $a^n - b^n$, Ann. of Math. (2), 5 (1904), 173-180.

3. J. Goldhaber and G. Ehrlich, "Algebra", Macmillan, London, 1970, pp. 91-92.

4. K. Kubota, On a conjecture of Morgan Ward II, Acta Arith. 33 (1977), 29-48.

5. R. Laxton, Linear p-adic recurrences, Quart. J. Math. Oxford Ser. (2), 19 (1968), 305-311.

6. K. Mahler, Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, Akad. Wetensch. Amsterdam, Proc. 38 (1935), 50-60.

7. K. Mahler, A remark on recursive sequences, J. Math. Sci. 1 (1966), 12-17.

8. M. Mignotte, Suites récurrentes linéaires, Sém. Delange-Pisot-Poitou, 15e année, 1973-4, Fasc. 2, No. G14, 1-9.

9. M. Mignotte, A note on linear recursive sequences, J. Austr. Math. Soc. Ser. A, 20 (1975), 242-244.

10. G. Polya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, J. Reine Angew. Math., 151 (1920), 1-31.

11. A. Schinzel, On two theorems of Gelfond and some of their applications, Acta Arith. 13 (1967/68), 177-236.

12. A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, J. Reine Angew. Math. 268/269 (1974), 27-33.

13. T. Shorey and R. Tijdeman, On the greatest prime factor of polynomials at integer points, Comp. Math. 33 (1976), 187-195.

14. C. Stewart, Primitive divisors of Lucas and Lehmer Numbers, in "Advances in Transcendence Theory", Academic Press, London, 1978.

15. R. Strassman, Uber der Wertevorrat von Potenzreihen in Gebiet det p-adischen Zahlen, J. Reine Angew. Math. 159 (1928), 13-28.

16. R. Tijdeman, On the number of zeros of general exponential polynomials, Indag. Math. 33 (1971), 1-7.

17. P. Turan, "Eine neue Methode in der Analysis und deren Anwendungen, Akadémiai Kiadó, Budapest, 1953.

18. A. van der Poorten, Zeros of p-adic exponential polynomials, Akad. van Wetensch. Amsterdam, Proc. Ser. A 79 (1976), 46-49.

19. A. van der Poorten, Linear forms in logarithms in the p-adic case, in "Advances in Transcendence Theory", Academic Press, London, 1978.

20. M. Waldschmidt, Propriétés arithmétiques des valeurs de fonctions meromorphes algébriquement indépendantes, Acta Arith. 23 (1973), 19-88.

21. M. Waldschmidt, "Nombres Transcendants", Lecture Notes in Math. No. 402, Springer, Berlin, 1974, p. 173.